David Chaum presenting at the Odtü Blockchain Days Conference

Sun, Mar 10, 2024. 2:00PM UTC

SPEAKERS

David Chaum, Video Narration (David Chaum)

David Chaum 00:01
Okay, great. So it's such a pleasure to be here with with everyone today. You know, I have kind of an academic origin. And I would like to share a bit of that with you, and show you how that led to the emergence of the XX Network. And there's a lot of other things that I've been working on that are related, and I'd like to share some of that with you as well.

David Chaum 00:43
So let's just see if I can share my screen with you. Yes, so there's my website, chaum.com. And... there's a bunch of different projects here, and I'd like to go through them a bit, to give you a sense of what I've been doing over these years and where XX Network came from.

David Chaum 01:21
So I was a graduate student at Berkeley, UC Berkeley, perhaps you've heard of it, and I think it's probably one of the best, maybe the best public university in the world. It's not private, it's public. And they gave me a like a Regents four year fellowships. So that was kind of nice. And I was a graduate student in computer science. And some of my office mates and colleagues were people that you've heard of, like, Eric Schmidt, from Google was my office mate, and Bill Joy was there around the corner. And the Berkeley software distribution was something that my professor made happen and I was involved in, to a certain extent, as were they.

David Chaum 02:21
So back in those days, this was in the late 1970s, if you can imagine that, we didn't really have the web or any of that, and I had this vision for how the future would unfold. And I realised that everybody would be using computers for everything, and that they'd be carrying around little computers in their pockets, you know. And I realised that there were fundamentally two different ways that we could move into that world.

David Chaum 03:12
One way, was by copying the current ideas about how information is stored and maintained, and how people have to identify themselves constantly to protect society, and that everything should be somehow traceable by governments, and so forth. And so individuals as the data subjects, and I had this epiphany, this idea this, like, it just occurred to me: "Wow, maybe there's a different way to do it!" And that way would be - I like to call it completely inside out.

David Chaum 04:00
So in other words, instead of companies and government being able to see everything about you, and keep the data about you, and you always identifying yourself to them, you could hold all of this information yourself, prevent them from linking together what you're doing and seeing you online. And (which we'll come back to) and then when there is a legitimate query or question from society, government organisation, a company what have you to you, that you wish to answer, then you should be able to prove in zero knowledge that your answer is correct, without revealing more than that. And this is what I called a new paradigm for individuals in the information age.

David Chaum 05:06
And I think many of you are university students. And I want to tell you that while I was a graduate student, it sounded like a very big idea. But I put it forward. And it eventually reached mass awareness. And let me just show you back to the sharing of the screen. That here is this Scientific American article: "Achieving Electronic Privacy."

David Chaum 05:46
This article explained how to do it - in Scientific American is kind of a big deal. In those days, the articles were about 3500 words, and they were quite important. So let me encourage you to try to live up to your... if you have a vision or dreams, go for it. You know, back in the late 70s, early 80s, it was a much more optimistic time. But I don't think that you should just be afraid to act like it's an optimistic world. Because we are at a very flexible kind of inflection point in the history of civilization, we could go a lot of different directions from here. And no one really knows exactly which one, and if we don't do something, we'll get sort-of the default direction, and that does not look too good.

David Chaum 07:11
So let me talk about mixing, briefly, and we're gonna show you video. So one of the things you know, so I was a graduate student at Berkeley, and I was reading a lot of stuff and tried to think deeply about this new approach that I had and what it could mean. And I found this publication from the RAND Corporation by a guy named Paul Baran. And he basically said that traffic analysis, which is what they used to call metadata, snooping, was by far and away the most effective way to spy on people.

David Chaum 08:03
And that instead of breaking codes, which is a lot of work, what's often done - it was easier, and you get more data, and it's easier to analyse, and better quality data - is you study who talks to whom and when. People don't lie about that, and the timing of those messages is important. In fact, I went over to the library, the Doe library of Berkeley, and they had the Congressional Record books on the shelf they are in, you could see that the US Congress had asked the CIA to explain one of their covert operations, and they chose the coup in in Chile. And so there was a congressional testimony by the CIA explaining how they did this. And how they did it was traffic analysis.

David Chaum 08:54
They basically planted some software in the phone, central exchange computer of the presidential complex in Chile, and it would call back to Washington DC every night and tell them who talked to whom and when, and how long the call - not anything about what was said. And it was that data which they analysed, and were able to then find out who and how to take over the country kind of surgically,

which they did, there was a very quick coup and very effective and Allende was deposed and so that goes to show you how powerful traffic analysis is.

David Chaum 09:43
And when you want to do mass surveillance, it's even more powerful because it distils the amount of data that you need and people don't lie about the data, mislead you with what they say and, and so forth. And so, I had this vision for turning the informational life of people inside out, as I mentioned, and so a key part of it was solving the traffic analysis problem. Because if someone could see everywhere you go and when, then they could tie together all this stuff and spy on you. And so that had to be solved. And so I came up with a solution to it. It's one of the three technologies that I developed to show that you could turn in the informational.... do this new paradigm they reported in the Scientific American article.

David Chaum 10:50
So how do you solve the traffic analysis problem? Well, mixing. And mixing is a very simple thing. But it's a very powerful thing. And it just says that, when you send a message to someone, it doesn't go straight from your IP address to their IP address. Rather, you send it to a single IP address that everyone sends all their messages to, then that node, (maybe an XX Network node) takes those messages and reorders them, changes the encryption and sends them to the next node. And that node does a very similar thing, it takes all those messages, reorders them randomly, and changes the encryption outputs them to the next node. And so in XX Network, we use five nodes. And it's, it's extremely optimised. And that's the thing about mixing.

David Chaum 12:05
You know, mixing is not a one size fits all, just like computing isn't. Maybe you've learned that (that's what I learned in computer science school.) You know, there's no single computer architecture that's best for everything. That's why we need AI coprocessors and arithmetic units, you know, whatever... all kinds of different computers for different purposes. And it's the same thing with mixing. So XX Network is optimised for transactions, which is a very 'lowest common denominator' for a lot of applications. You can make mixing for a lot of other things. And I'll give you a couple of examples. But they're more specialised and other people have done that. Or you could do a poor job of mixing with three hops, which is kind of an embarrassment and it's a kind of egregious, I think scam.

David Chaum 13:01
And then you're basically allowing people with a lot of resources to trace you need more than three hops. And so in XX Network, we have we're running currently, five hops, every half second, we send a batch through and it travels around the world through five nodes in, you can look at the dashboard in you know, very, very quickly in a second or so... couple seconds. So, let's can we run that video?

Video Narration (David Chaum): 13:36
Suppose Alice wants to send a message to Bob, but she doesn't want anyone to know that the two of them are communicating. Message content can easily be protected by so-called end-to-end encryption. But this does not protect the information about who's talking to whom and when - the metadata, which is increasingly recognised as far more revealing and more challenging to protect.

Video Narration (David Chaum): 14:00
Each member of a team of nodes in order to protect the metadata successively shuffles the batch of encrypted messages using its container of secretly arranged tubes and sending the messages without delay through to the next team member. Even just a single node can keep senders from being linked to recipients. Alice also gets a receipt informing her confidentially that her message was provided to Bob. Team members then destroy their secret pattern of tubes making way for a new team ready for a new batch.

Video Narration (David Chaum): 14:34
Earlier each node is chosen independently as a kind of random secret key - which input to to connect to which output tube. Elixxirs breakthrough (over the type of messaging I open sourced in the 80s) is a way that enables almost all the work to be done well in advance, yielding the only known way to provide real time metadata protection smartphone-to-smartphones. Elixxir, thus, is able to uniquely provide a new ultimate metadata level protection of confidentiality in all your online communications and payments for the first time giving you a protected sphere, protecting your digital world today and your digital future.

David Chaum 15:23
Great. So you see, one of the key things in the mixing that we have been running at XX Network is this pre-computation. And that's a real breakthrough, because that's what allows a node, when it receives, say, 1000 messages in a batch, to only have to do almost no computation to change the encryption. It's just a single multiply. And so the node can very quickly process the message and send it on. So this requires a special blockchain that we develop in XX Network that lets the team of nodes be chosen randomly by the consensus, but then do the pre-computation. And with the staking, they assert that they're ready to do a round and they're assigned a round, and then they do it. And if they succeed, then they they benefit with incentives.

David Chaum 16:25
So it's a really nice way to implement something that's very much needed, which is mixing for transactions. Now, there's some new kinds of mixing that have come up. And it turns out, if you look, Worldcoin has a big privacy problem. And that has to do with the scanning of biometric information and how that could be leaked. And I have found a solution to that, which is called Zanzibar. And recently, they are backing us to build a prototype of it. Well, that's all based on a new kind of mixing, a special kind of mixing, which we're building into XX Network.

David Chaum 17:12
And there's a lot of other kinds of mixing for privacy and payments that we're also building in. And so the cMixx+ will be something that a lot of privacy protecting systems around the world, will have to be using for all their transactions. And that will really be great for the network traffic, because the more traffic in privacy, the better.

David Chaum 17:39
Let me tell you real quickly about a couple of crazy things that happened to me personally, I broke the code, that was used by Swift, in these little blue boxes to protect all the Swift transactions that came in from the Swift headquarters to the banks, and the authentication and privacy and I broke it. You know, we say "up one side and down the other" and use differential cryptanalysis before it was public. And, the reason I mentioned this to you, and you can read about it, but that is kind of a big deal. A

government like that was used to spying on all the Swift transactions, it's kind of hard for them to give up on having access to that information.

David Chaum 18:30
I'd like to share with you something else that I did. And I urge you to go to my website and look at the Multi-Party Computation work. And you'll see that recently, I got all these awards for that - best paper in the last 30 years of theoretical computer science - and so on, because it's a very fundamental result. And if you have a theoretical inclination, I would urge you to try to follow it because there is nothing more thrilling in a professional sense than to make a real breakthrough on a theoretical front. This was just a standout event in my professional life. And I guess I should also point out a couple of things real quick.

David Chaum 19:27
That is that, I would like to tell you that, also when I was at Berkeley, in this vein, I also invented blockchain and I don't want to sound like Al Gore(!). But if you go here and you look at the publications, and you go to down to 'Computer systems established...', you'll see here that's my dissertation at Berkeley, which shows how to build a blockchain. But there's also an article here "On the origins and variations of blockchain technologies", that is a report that shows that this blockchain that I wrote the pseudocode for in '82, had all the elements of modern blockchains, except for the proof-of-work, which is... so I wanted to point that out.

David Chaum 20:19
And also this IACR. That's the International Association for Cryptologic Research. And I founded that when I was at Berkeley. Because at that time, (you can read about it on the on the ICR. panel there on the website), because the head of the National Security Agency, the United States, said that you couldn't have conferences on cryptography anymore. Just because of national security. So just as I was realising how fundamentally important privacy is, towards the good way to move into the information age, this guy was saying, "you can't do any public research on cryptography." So at risk in spending the rest of my life in jail, I organised the conference on cryptography, which he said, you know, he would imprison people for and throw the whole book at, as we say.

David Chaum 21:25
So I know it's a different time now, for you, people at the university, and even in business, but I think it's important that we be true to our ideals. And, let's go for it. If you're interested in helping with some of this stuff. I hope you'll support XX Network. And if you're interested in some of these things on my website, please reach out to me. I'm always happy to work with students. And so thanks very much for the opportunity to speak to you today. I hope you have a great rest of your conference.